



## **IP Multicast Command Reference, Cisco IOS XE Release 3SE (Catalyst 3650 Switch)**

**First Published:** October 10, 2013

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

Text Part Number: OL-30713-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### Preface

#### Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

---

### CHAPTER 1

#### Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 4

CLI Error Messages 4

Configuration Logging 5

How to Use the CLI to Configure Features 5

Configuring the Command History 5

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 9

Editing Command Lines That Wrap 10

Searching and Filtering Output of show and more Commands 11

Accessing the CLI on a Switch Stack 12

Accessing the CLI Through a Console Connection or Through Telnet 12

---

### CHAPTER 2

#### IP Multicast Commands 13

cache-memory-max 15

clear ip mfib counters	16
clear ip mroute	17
ip igmp filter	19
ip igmp max-groups	20
ip igmp profile	22
ip igmp snooping	24
ip igmp snooping last-member-query-count	25
ip igmp snooping querier	27
ip igmp snooping report-suppression	29
ip igmp snooping vlan mrouter	30
ip igmp snooping vlan static	31
ip multicast auto-enable	33
ip multicast vlan	34
ip pim accept-register	35
ip pim bsr-candidate	36
ip pim rp-candidate	38
ip pim send-rp-announce	40
ip pim spt-threshold	42
match message-type	43
match service-type	44
match service-instance	45
mrinfo	46
redistribute mdns-sd	48
service-list mdns-sd	49
service-policy-query	51
service-routing mdns-sd	52
service-policy	53
show ip igmp filter	54
show ip igmp profile	55
show ip igmp snooping	56
show ip igmp snooping groups	58
show ip igmp snooping igmpv2-tracking	60
show ip igmp snooping mrouter	61
show ip igmp snooping querier	62
show ip igmp snooping wireless mcast-spi-count	64

show ip igmp snooping wireless mgid	65
show ip pim autorp	66
show ip pim bsr-router	67
show ip pim bsr	68
show ip pim tunnel	69
show mdns cache	71
show mdns requests	73
show mdns statistics	74
show platform ip multicast	75
wireless mdns-bridging	82
wireless multicast	83





## Preface

- [Document Conventions](#), page vii
- [Related Documentation](#), page ix
- [Obtaining Documentation and Submitting a Service Request](#), page ix

## Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination <b>^D</b> or <b>Ctrl-D</b> means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<b>bold font</b>	Commands and keywords and user-entered text appear in <b>bold font</b> .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <i>courier font</i> .
<b>Bold Courier font</b>	<b>Bold Courier font</b> indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x   y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Description
{x   y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y   z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

### Reader Alert Conventions

This document may use the following conventions for reader alerts:



#### Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



#### Tip

Means *the following information will help you solve a problem*.



#### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



#### Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



#### Warning

Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.



## Related Documentation

**Note**

---

Before installing or upgrading the switch, refer to the switch release notes.

---

- Cisco Catalyst 3650 Switch documentation, located at:  
[http://www.cisco.com/go/cat3650\\_docs](http://www.cisco.com/go/cat3650_docs)
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:  
[http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html)
- Error Message Decoder, located at:  
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





## Using the Command-Line Interface

---

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 5](#)

## Information About Using the Command-Line Interface

### Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Switch>	Enter <b>logout</b> or <b>quit</b> .	Use this mode to <ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display system information.</li> </ul>
Privileged EXEC	While in user EXEC mode, enter the <b>enable</b> command.	Switch#	Enter <b>disable</b> to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the <b>configure</b> command.	Switch(config)#	To exit to privileged EXEC mode, enter <b>exit</b> or <b>end</b> , or press <b>Ctrl-Z</b> .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the <b>vlan</b> <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the <b>exit</b> command. To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the <b>interface</b> command (with a specific interface).	Switch(config-if)#	To exit to global configuration mode, enter <b>exit</b> . To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the <b>line vty</b> or <b>line console</b> command.	Switch(config-line)#	To exit to global configuration mode, enter <b>exit</b> .  To return to privileged EXEC mode, press <b>Ctrl-Z</b> or enter <b>end</b> .	Use this mode to configure parameters for the terminal line.

## Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

### SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>help</b>  <b>Example:</b> Switch# <b>help</b>	Obtains a brief description of the help system in any command mode.
<b>Step 2</b>	<i>abbreviated-command-entry ?</i>  <b>Example:</b> Switch# <b>di?</b> dir disable disconnect	Obtains a list of commands that begin with a particular character string.
<b>Step 3</b>	<i>abbreviated-command-entry &lt;Tab&gt;</i>  <b>Example:</b> Switch# <b>sh conf&lt;tab&gt;</b> Switch# <b>show configuration</b>	Completes a partial command name.

	Command or Action	Purpose
Step 4	?  <b>Example:</b> Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command</i> ?  <b>Example:</b> Switch> <b>show</b> ?	Lists the associated keywords for a command.
Step 6	<i>command keyword</i> ?  <b>Example:</b> Switch(config)# <b>cdp holdtime</b> ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

## Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

## No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

## CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

**Table 2: Common CLI Error Messages**

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark.  The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode.  The possible keywords that you can enter with the command appear.

## Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.




---

**Note** Only CLI or HTTP changes are logged.

---

## How to Use the CLI to Configure Features

### Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

## Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

### SUMMARY STEPS

1. **terminal history** [*size number-of-lines*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal history</b> [ <i>size number-of-lines</i> ]  <b>Example:</b> Switch# <b>terminal history size 200</b>	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

## Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

### SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>Ctrl-P</b> or use the <b>up arrow</b> key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
<b>Step 2</b>	<b>Ctrl-N</b> or use the <b>down arrow</b> key	Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the up arrow key. Repeat the key sequence to recall successively more recent commands.



	Command or Action	Purpose
<b>Step 3</b>	<b>show history</b>  <b>Example:</b> Switch# <code>show history</code>	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the <b>terminal history</b> global configuration command and the <b>history</b> line configuration command.

## Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

### SUMMARY STEPS

1. `terminal no history`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal no history</b>  <b>Example:</b> Switch# <code>terminal no history</code>	Disables the feature during the current terminal session in privileged EXEC mode.

## Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenble it.

### SUMMARY STEPS

1. `terminal editing`
2. `terminal no editing`

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>terminal editing</b>  <b>Example:</b> Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>terminal no editing</b>  <b>Example:</b> Switch# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

## Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.


**Note**

The arrow keys function only on ANSI-compatible terminals such as VT100s.

**Table 3: Editing Commands**

Editing Commands	Description
<b>Ctrl-B</b> or use the <b>left arrow</b> key	Moves the cursor back one character.
<b>Ctrl-F</b> or use the <b>right arrow</b> key	Moves the cursor forward one character.
<b>Ctrl-A</b>	Moves the cursor to the beginning of the command line.
<b>Ctrl-E</b>	Moves the cursor to the end of the command line.
<b>Esc B</b>	Moves the cursor back one word.
<b>Esc F</b>	Moves the cursor forward one word.
<b>Ctrl-T</b>	Transposes the character to the left of the cursor with the character located at the cursor.
<b>Delete</b> or <b>Backspace</b> key	Erases the character to the left of the cursor.
<b>Ctrl-D</b>	Deletes the character at the cursor.
<b>Ctrl-K</b>	Deletes all characters from the cursor to the end of the command line.
<b>Ctrl-U</b> or <b>Ctrl-X</b>	Deletes all characters from the cursor to the beginning of the command line.
<b>Ctrl-W</b>	Deletes the word to the left of the cursor.
<b>Esc D</b>	Deletes from the cursor to the end of the word.
<b>Esc C</b>	Capitalizes at the cursor.
<b>Esc L</b>	Changes the word at the cursor to lowercase.
<b>Esc U</b>	Capitalizes letters from the cursor to the end of the word.

<b>Ctrl-V</b> or <b>Esc Q</b>	Designates a particular keystroke as an executable command, perhaps as a shortcut.
<b>Return</b> key	Scrolls down a line or screen on displays that are longer than the terminal screen can display.  <b>Note</b> The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including <b>show</b> command output. You can use the <b>Return</b> and <b>Space</b> bar keystrokes whenever you see the More prompt.
<b>Space</b> bar	Scrolls down one screen.
<b>Ctrl-L</b> or <b>Ctrl-R</b>	Redisplays the current command line if the switch suddenly sends a message to your screen.

## Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.



### Note

The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

## SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>access-list</b>  <b>Example:</b> Switch(config)# <b>access-list 101 permit tcp</b>	Displays the global configuration command entry that extends beyond one line.  When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the

	Command or Action	Purpose
	<pre>10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	<p><b>Ctrl-A</b></p> <p><b>Example:</b></p> <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	<p>Checks the complete syntax.</p> <p>The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.</p>
Step 3	<b>Return key</b>	<p>Execute the commands.</p> <p>The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the <b>terminal width</b> privileged EXEC command to set the width of your terminal.</p> <p>Use line wrapping with the command history feature to recall and modify previous complex command entries.</p>

## Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

### SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>{show   more} command   {begin   include   exclude} regular-expression</pre> <p><b>Example:</b></p> <pre>Switch# show interfaces   include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	<p>Searches and filters the output.</p> <p>Expressions are case sensitive. For example, if you enter <b>  exclude output</b>, the lines that contain <b>output</b> are not displayed, but the lines that contain <b>output</b> appear.</p>

## Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.

**Note**

---

We recommend using one CLI session when managing the switch stack.

---

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug the standby switch, use the **session standby ios** privileged EXEC command from the active switch to access the IOS console of the standby switch. To debug a specific stack member, use the **session switch stack-member-number** privileged EXEC command from the active switch to access the diagnostic shell of the stack member. For more information about these commands, see the switch command reference.

## Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
  - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
  - The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



## IP Multicast Commands

---

- [cache-memory-max](#), page 15
- [clear ip mfib counters](#), page 16
- [clear ip mroute](#), page 17
- [ip igmp filter](#), page 19
- [ip igmp max-groups](#), page 20
- [ip igmp profile](#), page 22
- [ip igmp snooping](#), page 24
- [ip igmp snooping last-member-query-count](#), page 25
- [ip igmp snooping querier](#), page 27
- [ip igmp snooping report-suppression](#), page 29
- [ip igmp snooping vlan mrouter](#), page 30
- [ip igmp snooping vlan static](#), page 31
- [ip multicast auto-enable](#), page 33
- [ip multicast vlan](#), page 34
- [ip pim accept-register](#), page 35
- [ip pim bsr-candidate](#), page 36
- [ip pim rp-candidate](#), page 38
- [ip pim send-rp-announce](#), page 40
- [ip pim spt-threshold](#), page 42
- [match message-type](#), page 43
- [match service-type](#), page 44
- [match service-instance](#), page 45
- [mrintfo](#), page 46
- [redistribute mdns-sd](#), page 48

- [service-list mdns-sd](#), page 49
- [service-policy-query](#), page 51
- [service-routing mdns-sd](#), page 52
- [service-policy](#), page 53
- [show ip igmp filter](#), page 54
- [show ip igmp profile](#), page 55
- [show ip igmp snooping](#), page 56
- [show ip igmp snooping groups](#), page 58
- [show ip igmp snooping igmpv2-tracking](#), page 60
- [show ip igmp snooping mrouter](#), page 61
- [show ip igmp snooping querier](#), page 62
- [show ip igmp snooping wireless mcast-spi-count](#), page 64
- [show ip igmp snooping wireless mgid](#), page 65
- [show ip pim autorp](#), page 66
- [show ip pim bsr-router](#), page 67
- [show ip pim bsr](#), page 68
- [show ip pim tunnel](#), page 69
- [show mdns cache](#), page 71
- [show mdns requests](#), page 73
- [show mdns statistics](#), page 74
- [show platform ip multicast](#), page 75
- [wireless mdns-bridging](#), page 82
- [wireless multicast](#), page 83



# cache-memory-max

To set a percentage of the system memory for cache, use the **cache-memory-max** command. To remove a percentage of system memory for cache, use the **no** form of this command.

**cache-memory-max** *cache-config-percentage*

**no cache-memory-max** *cache-config-percentage*

## Syntax Description

*cache-config-percentage*

A percentage of the system memory for cache.

## Command Default

10 percent.

## Command Modes

mDNS configuration

## Command History

### Release

Cisco IOS XE 3.3SE

### Modification

This command was introduced.

## Usage Guidelines

The number of services learned in a network could be large, so there is an upper limit on the amount of cache memory that can be used. The memory is set by default to a maximum of 10 percent of the system memory.



### Note

You can override the default value by using this command.

When you try to add new records, and the cache is full, the records in the cache that are close to expiring are deleted to provide space for the new records.

## Examples

This example sets 20 percent of the system memory for cache:

```
Switch(config-mdns)# cache-memory-max 20
```

## clear ip mfib counters

To clear all active IPv4 multicast forwarding information base (MFIB) traffic counters, use the **clear ip mfib counters** privileged exec command.

```
clear ip mfib [global | vrf *] counters [group-address] [hostname | source-address]
```

### Syntax Description

<b>global</b>	(Optional) Resets the IP multicast forwarding information base cache to the global default configuration.
<b>vrf *</b>	(Optional) Clears the IP multicast forwarding information base cache for all VPN routing and forwarding instances.
<i>group-address</i>	(Optional) Limits the active multicast forwarding information base (MFIB) traffic counters to the indicated group address.
<i>hostname</i>   <i>source-address</i>	(Optional) Limits the active multicast forwarding information base (MFIB) traffic counters to the indicated host name or source address.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

None

### Examples

The following example shows how to reset all active MFIB traffic counters for all multicast tables:

```
Switch# clear ip mfib counters
```

The following example shows how to reset the IP multicast forwarding information base cache counters to the global default configuration:

```
Switch# clear ip mfib global counters
```

The following example shows how to clear the IP multicast forwarding information base cache for the all VPN routing and forwarding instances:

```
Switch# clear ip mfib vrf * counters
```

# clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** privileged EXEC command.

```
clear ip mroute [vrf vrf-name]{* | ip-address | group-address}[hostname | source-address]
```

## Syntax Description

<i>vrf vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
*	Specifies all Multicast routes.
<i>ip-address</i>	Multicast routes for the IP address.
<i>group-address</i>	Multicast routes for the group address.
<i>hostname</i>	(Optional) Multicast routes for the host name.
<i>source-address</i>	(Optional) Multicast routes for the source address.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

## Examples

The following example shows how to delete all entries from the IP multicast routing table:

```
Switch# clear ip mroute *
```

The following example shows how to delete all sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
Switch# clear ip mroute 224.2.205.42 228.3.0.0
```

## ip igmp filter

To control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface, use the **ip igmp filter** interface configuration command on the switch stack or on a standalone switch. To remove the specified profile from the interface, use the **no** form of this command.

**ip igmp filter** *profile number*

**no ip igmp filter**

<b>Syntax Description</b>	<i>profile number</i>	The IGMP profile number to be applied. The range is 1 to 4294967295.
---------------------------	-----------------------	--

**Command Default** No IGMP filters are applied.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

**Examples** You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

## ip igmp max-groups

To set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table, use the **ip igmp max-groups** interface configuration command on the switch stack or on a standalone switch. To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

```
ip igmp max-groups {max number | action { deny | replace}}
```

```
no ip igmp max-groups {max number | action}
```

### Syntax Description

<i>max number</i>	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
<b>action deny</b>	Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.
<b>action replace</b>	Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the IGMP snooping forwarding table.

### Command Default

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

### Command Modes

Interface configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged

out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.

- If you configure the throttling action as `replace` and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the `ip igmp max-groups {deny | replace}` command has no effect.

## Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# ip igmp max-groups 25
```

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the `show running-config` privileged EXEC command and by specifying an interface.

## ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command on the switch stack or on a standalone switch. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

**ip igmp profile** *profile number*

**no ip igmp profile** *profile number*

### Syntax Description

<i>profile number</i>	The IGMP profile number being configured. The range is from 1 to 4294967295.
-----------------------	--

### Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**—Specifies that matching addresses are denied; this is the default condition.
- **exit**—Exits from igmp-profile configuration mode.
- **no**—Negates a command or resets to its defaults.
- **permit**—Specifies that matching addresses are permitted.
- **range**—Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.



## Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

## ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

**ip igmp snooping** [*vlan vlan-id*]

**no ip igmp snooping** [*vlan vlan-id*]

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
----------------------------	--

### Command Default

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

### Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of the command.

**ip igmp snooping** [*vlan vlan-id*] **last-member-query-count** *count*

**no ip igmp snooping** [*vlan vlan-id*] **last-member-query-count** *count*

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Sets the count value on a specific VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
<i>count</i>	The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

### Command Default

A query is sent every 2 milliseconds.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response to the last-member queries are received before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.



#### Note

Do not set the count to 1 because the loss of a single packet (the query packet from the switch to the host or the report packet from the host to the switch) may result in traffic forwarding being stopped even if there is still a receiver. Traffic continues to be forwarded after the next general query is sent by the switch, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last-member-query-interval (LMQI) value when the switch is processing more than one leave within an LMQI. In this case, the average leave latency is

determined by the  $(\text{count} + 0.5) * \text{LMQI}$ . The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

### Examples

The following example sets the last member query count to 5:

```
Switch(config)# ip igmp snooping last-member-query-count 5
```

## ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

**ip igmp snooping** [*vlan vlan-id*] **querier** [*address ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {*count count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

**no ip igmp snooping** [*vlan vlan-id*] **querier** [*address* | **max-response-time** | **query-interval** | **tcn query** {*count* | **interval**} | **timer expiry** | **version**]

### Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
<b>address</b> <i>ip-address</i>	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
<b>max-response-time</b> <i>response-time</i>	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
<b>query-interval</b> <i>interval-count</i>	(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.
<b>tcn query</b>	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
<b>count</b> <i>count</i>	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
<b>interval</b> <i>interval</i>	Sets the TCN query interval time. The range is 1 to 255.
<b>timer expiry</b> <i>expiry-time</i>	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.
<b>version</b> <i>version</i>	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.

### Command Default

The IGMP snooping querier feature is globally disabled on the switch.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

### Command Modes

Global configuration

**Command History**

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines**

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2) but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the max-response-time value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the max-response-time value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

**Examples**

This example shows how to globally enable the IGMP snooping querier feature:

```
Switch(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Switch(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Switch(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch(config)# ip igmp snooping querier timer expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

# ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the switch stack or on a standalone switch. To disable IGMP report suppression and to forward all IGMP reports to multicast routers, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

**Syntax Description** This command has no arguments or keywords.

**Command Default** IGMP report suppression is enabled.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

**Examples** This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the switch stack or on a standalone switch. To return to the default settings, use the **no** form of this command.

**Command Default** By default, there are no multicast router ports.

**Command Modes** Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping. The configuration is saved in NVRAM.

**Examples** This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.



## ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to remove ports specified as members of a static multicast group.

**ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-id*

**no ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-id*

### Syntax Description

<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
<i>ip-address</i>	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
<b>interface</b> <i>interface-id</i>	Specifies the interface of the member port. The <i>interface-id</i> value has these options: <ul style="list-style-type: none"> <li><i>fastethernet interface number</i>—A Fast Ethernet IEEE 802.3 interface.</li> <li><i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface.</li> <li><i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface.</li> <li><i>port-channel interface number</i>—A channel interface. The range is 0 to 128.</li> </ul>

### Command Default

By default, there are no ports statically configured as members of a multicast group.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping. The configuration is saved in NVRAM.

## Examples

This example shows how to statically configure a host on an interface:

```
Switch(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
Configuring port gigabitEthernet1/0/1 on group 224.2.4.12
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of the command.

**ip multicast auto-enable**

**no ip multicast auto-enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** None

**Examples** This example shows how to enable authentication, authorization, and accounting (AAA) on IP multicast:

```
Switch(config)# ip multicast auto-enable
```

## ip multicast vlan

To configure IP multicast on a single VLAN, use the **ip multicast vlan** command in global configuration mode. To remove the VLAN from the WLAN, use the **no** form of the command.

**ip multicast vlan** {*vlan-name* | *vlan-id*}

**no ip multicast vlan** {*vlan-name* | *vlan-id*}

### Syntax Description

<i>vlan-name</i>	Specifies the VLAN name.
<i>vlan-id</i>	Specifies the VLAN ID.

### Command Default

Disabled.

### Command Modes

WLAN configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

None

### Examples

This example configures `vlan_id01` as a multicast VLAN.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan 1
Switch(config-wlan)# ip multicast vlan vlan_id01
```

## ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

```
ip pim [vrf vrf-name ] accept-register {list access-list}
```

```
no ip pim [vrf vrf-name ] accept-register
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
<b>list</b> <i>access-list</i>	Specifies the <i>access-list</i> argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100 to 199 and an expanded range of 2000 to 2699. An IP-named access list can also be used.

### Command Default

No PIM register filters are configured.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list provided for the **ip pim accept-register** command should only filter on IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is desired, use the **ip multicast boundary** command instead.

### Examples

The following example shows how to permit register packets for any source address sending to any group range, with the exception of source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). These are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers or switches.

```
Switch(config)# ip pim accept-register list ssm-range
Switch(config)# ip access-list extended ssm-range
Switch(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
Switch(config-ext-nacl)# permit ip any any
```

## ip pim bsr-candidate

To configure the switch to be a candidate BSR, use the **ip pim bsr-candidate** command in global configuration mode. To remove the switch as a candidate BSR, use the **no** form of this command.

**ip pim** [*vrf vrf-name*] **bsr-candidate** *interface-id* [*hash-mask-length*] [*priority*]

**no ip pim** [*vrf vrf-name*] **bsr-candidate**

### Syntax Description

<i>vrf vrf-name</i>	(Optional) Configures the switch to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
<i>interface-id</i>	ID of the interface on this switch from which the BSR address is derived to make it a candidate. This interface must be enabled for Protocol Independent Multicast (PIM) using the <b>ip pim</b> command. Valid interfaces include physical ports, port channels, and VLANs.
<i>hash-mask-length</i>	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
<i>priority</i>	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.

### Command Default

The switch is not configured to announce itself as a candidate BSR.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the switch to send BSR messages to all of its PIM neighbors, with the address of the designated interface as the BSR address.

This command should be configured on backbone switches that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) switches unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so no preexisting IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each switch that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Cisco switches always accept and process BSR messages. There is no command to disable this function.

Cisco switches perform the following steps to determine which C-RP is used for a group:

- A longest match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP are found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
- If more than one BSR-learned C-RP have the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP return the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

### Examples

The following example shows how to configure the IP address of the switch on Gigabit Ethernet interface 1/0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Switch(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

## ip pim rp-candidate

To configure the switch to advertise itself to the BSR as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this switch as a C-RP, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
```

```
no ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
```

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
<i>interface-id</i>	ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.
<b>group-list</b> <i>access-list-number</i>	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

### Command Default

The switch is not configured to announce itself to the BSR as a PIMv2 C-RP.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

Use this command to configure the switch to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.

This command should be configured on backbone switches that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified by *interface-id* will be advertised as the C-RP address.

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list-number* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.



**Examples**

The following example shows how to configure the switch to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 1/0/1.

```
Switch(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

## ip pim send-rp-announce

To use Auto-RP to configure groups for which the switch will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this switch as an RP, use the **no** form of this command.

**ip pim** [*vrf vrf-name*] **send-rp-announce** *interface-id* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*]

**no ip pim** [*vrf vrf-name*] **send-rp-announce** *interface-id*

### Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Uses Auto-RP to configure groups for which the switch will act as a rendezvous point (RP) for the <i>vrf-name</i> argument.
<i>interface-id</i>	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.
<b>scope</b> <i>ttl-value</i>	Specifies the time-to-live (TTL) value in hops that limits the number of Auto-RP announcements. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.
<b>group-list</b> <i>access-list-number</i>	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.
<b>interval</b> <i>seconds</i>	(Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1 to 16383.

### Command Default

Auto-RP is disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

Enter this command on the switch that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the

well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

### Examples

The following example shows how to configure the switch to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the switch wants to be identified as RP is the IP address associated with Gigabit Ethernet interface 1/0/1 at an interval of 120 seconds:

```
Switch(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval  
120
```

## ip pim spt-threshold

To specify the threshold that must be reached before moving to shortest-path tree (spt), use the **ip pim spt-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

**ip pim** {*kbits* | **infinity**} [**group-list** *access-list*]

**no ip pim** {*kbits* | **infinity**} [**group-list** *access-list*]

### Syntax Description

<i>kbits</i>	The threshold that must be reached before moving to shortest-path tree (spt). 0 is the only valid entry even though the range is 0 to 4294967. A 0 entry always switches to the source-tree.
<b>infinity</b>	Specifies that all sources for the specified group use the shared tree, never switching to the source tree.
<b>group-list</b> <i>access-list</i>	(Optional) Specifies an access list number or a specific access list that you have created by name. If the value is 0 or if the <b>group-list</b> <i>access-list</i> option is not used, the threshold applies to all groups.

### Command Default

Switches to the PIM shortest-path tree (spt).

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

None

### Examples

The following example makes all sources for access list 16 use the shared tree:

```
Switch(config)# ip pim spt-threshold infinity group-list 16
```

# match message-type

To set the message type to match for a service list, use the **match message-type** command.

```
match message-type {announcement| any| query}
```

## Syntax Description

<b>announcement</b>	Allows only service advertisements or announcements for the device.
<b>any</b>	Allows any match type.
<b>query</b>	Allows only a query from the client for a certain device in the network.

## Command Default

None

## Command Modes

Service list configuration.

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny.



### Note

It is not possible to use the **match** command if you have used the **service-list mdns-sd service-list-name query** command. The **match** command can be used only for the **permit** or **deny** option.

## Examples

This example shows how to set the announcement message type to be matched:

```
Switch(config-mdns-sd-sl) # match message-type announcement
```

## match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

**match service-type** *line*

### Syntax Description

<i>line</i>	Regular expression to match service type in packets.
-------------	--

### Command Default

None

### Command Modes

Service list configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

### Examples

This example shows how to set the value of the mDNS service type string to match:

```
Switch(config-mdns-sd-sl)# match service-type _ipp._tcp
```

## match service-instance

To set the service instance to match for a service list, use the **match service-instance** command.

**match service-instance** *line*

### Syntax Description

<i>line</i>	Regular expression to match service instance in packets.
-------------	--

### Command Default

None

### Command Modes

Service list configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd service-list-name query** command. The **match** command can be used only for the **permit** or **deny** option.

### Examples

This example shows how to set the service instance to match:

```
Switch(config-mdns-sd-sl) # match service-instance servInst 1
```

# mrinfo

To query which neighboring multicast routers or multilayer switches are acting as peers, use the **mrinfo** command in user EXEC or privileged EXEC mode.

**mrinfo** [*vrf route-name*] [*hostname | address*][*interface-id*]

## Syntax Description

<i>vrf route-name</i>	(Optional) Specifies the VPN routing or forwarding instance.
<i>hostname   address</i>	(Optional) The Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
<i>interface-id</i>	(Optional) Specifies the interface ID.

## Command Default

The command is disabled.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers have supported responding to mrinfo requests since Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouterd software is the UNIX software that implements DVMRP.)

## Examples

The following is sample output from the **mrinfo** command:

```
Switch# mrinfo
vrf 192.0.1.0
192.31.7.37 (barnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```



**Note**

---

The flags indicate the following:

- P: prune-capable
  - M: mtrace-capable
  - S: Simple Network Management Protocol (SNMP)-capable
  - A: Auto-Rendezvous Point (RP)-capable
-

## redistribute mdns-sd

To redistribute services or service announcements across subnets, use the **redistribute mdns-sd** command. To disable redistribution of services or service announcements across subnets, use the **no** form of this command.

**redistribute mdns-sd**

**no redistribute mdns-sd**

This command has no arguments or keywords.

### Command Default

The redistribution of services or service announcements across subnets is disabled.

### Command Modes

mDNS configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

To redistribute service announcements across interfaces, use the **redistribute mdns-sd** command. This command sends out unsolicited announcements received on one interface to all of the other interfaces. The outgoing announcements are filtered as per the out-service policy defined for the interface or in absence of a per-interface service policy based on the global out-service policy.

In the absence of a redistribute option, services can be discovered by querying in a Layer 3 domain that is not local to the service provider.

### Examples

This example shows how to redistribute services or service announcements across subnets:

```
Switch(config-mdns) # redistribute mdns-sd
```



#### Note

If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

## service-list mdns-sd

To enter mDNS service discovery service-list mode on the switch, use the **service-list mdns-sd** command. To exit mDNS service discovery service-list mode, use the **no** form of the command.

**service-list mdns-sd** *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

**no service-list mdns-sd** *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

### Syntax Description

<i>service-list-name</i>	Name of the service list.
<b>permit</b> <i>sequence number</i>	Permits a filter on the service list to be applied to the sequence number.
<b>deny</b> <i>sequence number</i>	Denies a filter on the service list to be applied to the sequence number.
<b>query</b>	Associates a query for the service list name.

### Command Default

Disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

Service filters are modeled around access lists and route maps.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each has a permit or deny result. Evaluation of a service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action, permit or deny associated with the statement match is performed. Default action after scanning through the entire list will be to deny.

This command can be used to enter mDNS service discovery service-list mode.

In this mode you can:

- Create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number.

### Examples

This example shows how to create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number:

```
Switch(config)# service-list mdns-sd s11 permit 3
```

## service-policy-query

To configure service list query periodicity, use the **service-policy-query** command. To delete the configuration, use the **no** form of this command.

**service-policy-query** [*service-list-query-name service-list-query-periodicity*]

**no service-policy-query**

### Syntax Description

*service-list-query-name service-list-query-periodicity* (Optional) Configures the service list query periodicity.

### Command Default

Disabled.

### Command Modes

mDNS configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

As there are devices that do not send unsolicited announcements and to force learning of services and to keep them refreshed in the cache, this command contains an active query feature which ensures that services listed in the active query list will be queried.

### Examples

This example shows how to configure service list query periodicity:

```
Switch(config-mdns) # service-policy-query sl-query1 100
```

## service-routing mdns-sd

To enable mDNS gateway functionality for a device and enter multicast DNS configuration mode, use the **service-routing mdns-sd** command. To restore default settings and return to global config mode, enter the **no** form of the command.

**service-routing mdns-sd**

**no service-routing mdns-sd**

This command has no arguments or keywords.

### Command Default

Disabled.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

mDNS gateway functionality can only be enabled or disabled globally, not on a per-interface basis. The service filter policy and redistribution can be configured globally as well as on a per-interface basis. Any interface specific configuration overrides the global configuration.

### Examples

This example shows how to enable mDNS gateway functionality for a device and enter multicast DNS configuration mode:

```
Switch(config)# service-routing mdns-sd
```

# service-policy

To apply a filter on incoming or outgoing service discovery information on a service list, use the **service-policy** command. To remove the filter, use the **no** form of the command.

**service-policy** *service-policy-name* {**IN** | **OUT**}

**no service-policy** *service-policy-name* {**IN** | **OUT**}

## Syntax Description

<i>service-policy-name</i> <b>IN</b>	Applies a filter on incoming service discovery information.
<i>service-policy-name</i> <b>OUT</b>	Applies a filter on outgoing service discovery information.

## Command Default

Disabled.

## Command Modes

mDNS configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

The Switch intercepts mDNS packets. If they are mDNS messages destined to a wireless client (for example, the destination MAC is client's MAC address), and the client's mobility state is either local or foreign, the destination MAC address is overwritten with the client's MAC address and enqueues the packet to be sent out on the associated CAPWAP tunnel.

## Examples

This example applies a filter on incoming service discovery information on a service list:

```
Switch(config-mdns)# service-policy serv-poll IN
```

# show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the **show ip igmp filter** command in privileged EXEC command mode.

**show ip igmp** [*vrf vrf-name*] **filter**

## Syntax Description

<i>vrf vrf-name</i>	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
---------------------	--

## Command Default

IGMP filters are enabled by default.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

The **show ip igmp filter** command displays information about all filters defined on the switch.

## Examples

The following is sample output from the **show ip igmp filter** command:

```
Switch# show ip igmp filter
IGMP filter enabled
```



# show ip igmp profile

To display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** privileged EXEC command.

```
show ip igmp [vrf vrf-name] profile [profile number]
```

Syntax Description	
<i>vrf vrf-name</i>	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
<i>profile number</i>	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.

**Command Default** IGMP profiles undefined by default.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** None

**Examples** The following example shows the output of the **show ip igmp profile** privileged EXEC command for profile number 40 on the switch:

```
Switch# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
```

This example shows the output of the **show ip igmp profile** privileged EXEC command for all profiles configured on the switch:

```
Switch# show ip igmp profile

IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

# show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN, use the **show ip igmp snooping** command in user or privileged EXEC command mode.

**show ip igmp snooping** [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

## Syntax Description

<b>groups</b>	(Optional) Displays the IGMP snooping multicast table.
<b>mrouter</b>	(Optional) Displays the IGMP snooping multicast router ports.
<b>querier</b>	(Optional) Displays the configuration and operation information for the IGMP querier.
<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
<b>detail</b>	(Optional) Displays operational state information.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping. Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

## Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Switch# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression     : Enabled
TCN solicit query      : Disabled
TCN flood query count   : 2
```

```

Robustness variable      : 2
Last member query count  : 2
Last member query interval : 1000

```

```
Vlan 1:
```

```

-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable     : 2
Last member query count  : 2
Last member query interval : 1000

```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch:

```

Switch# show ip igmp snooping
Global IGMP Snooping configuration:
-----
IGMP snooping           : Enabled
IGMPv3 snooping (minimal) : Enabled
Report suppression      : Enabled
TCN solicit query       : Disabled
TCN flood query count   : 2
Robustness variable     : 2
Last member query count  : 2
Last member query interval : 1000

Vlan 1:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable     : 2
Last member query count  : 2
Last member query interval : 1000
Vlan 2:
-----
IGMP snooping           : Enabled
IGMPv2 immediate leave  : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable     : 2
Last member query count  : 2
Last member query interval : 1000
<output truncated>

```

# show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information, use the **show ip igmp snooping groups** privileged EXEC command.

```
show ip igmp snooping groups [vlan vlan-id] [[count] | ip_address]
```

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
<b>count</b>	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
<i>ip_address</i>	(Optional) Characteristics of the multicast group with the specified group IP address.

## Command Modes

Privileged EXEC  
User EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

## Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch:

```
Switch# show ip igmp snooping groups
Vlan      Group          Type          Version      Port List
-----
1         224.1.4.4      igmp          v2           Gi1/0/11
1         224.1.4.5      igmp          v2           Gi1/0/11
2         224.0.1.40     igmp          v2           Gi1/0/15
104      224.1.4.2      igmp          v2           Gi2/0/1, Gi2/0/2
104      224.1.4.3      igmp          v2           Gi2/0/1, Gi2/0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch:

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group          Type          Version      Port List
-----
104       224.1.4.2     igmp          v2           Gi2/0/1, Gi1/0/15
```

# show ip igmp snooping igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.


**Note**

The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

## show ip igmp snooping igmpv2-tracking

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

# show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** privileged EXEC command.

```
show ip igmp snooping mrouter [vlan vlan-id]
```

<b>Syntax Description</b>	<b>vlan <i>vlan-id</i></b> (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.				
<b>Command Modes</b>	User EXEC Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				

**Usage Guidelines**

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping. When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

**Examples**

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch:

```
Switch# show ip igmp snooping mrouter
Vlan      ports
----      -
  1       Gi2/0/1 (dynamic)
```

# show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier configured on a switch, use the **show ip igmp snooping querier** user EXEC command.

**show ip igmp snooping querier** [*vlan *vlan-id**] [*detail* ]

## Syntax Description

<b>vlan</b> <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
<b>detail</b>	(Optional) Displays detailed IGMP querier information.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the switch, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the switch querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the switch querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.



**Examples**

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11   v3                 Gi1/0/1
2         172.20.40.20   v2                 Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail
Vlan      IP Address      IGMP Version      Port
-----
1         1.1.1.1        v2                 Fa8/0/1
Global IGMP switch querier status
-----
admin state           : Enabled
admin version         : 2
source IP address     : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
Vlan 1: IGMP switch querier status
-----
elected querier is 1.1.1.1      on port Fa8/0/1
-----
admin state           : Enabled
admin version         : 2
source IP address     : 10.1.1.65
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count       : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

# show ip igmp snooping wireless mcast-spi-count

To display the statistics of the number of multicast stateful packet inspections (SPIs) per multicast group ID (MGID) sent to the switch, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

**show ip igmp snooping wireless mcast-spi-count**

This command has no arguments or keywords.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** None

**Examples** This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command:

```
Switch# show ip igmp snooping wireless mcast-spi-count
Stats for Mcast Client Add/Delete SPI Messages Sent to WCM
MGID    ADD MSGs      Del MSGs
-----
4160    1323          667
```

# show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

**show ip igmp snooping wireless mgid**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** None

**Examples** This is an example of output from the **show ip igmp snooping wireless mgid** command:

```
Switch# show ip igmp snooping wireless mgid

Total number of L2-MGIDs      = 0

Total number of MCAST MGIDs = 0

Wireless multicast is Enabled in the system
Vlan    bcast    nonip-mcast  mcast    mgid    Stdby Flags
1       Disabled  Disabled    Enabled   Disabled 0:0:1:0
25      Disabled  Disabled    Enabled   Disabled 0:0:1:0
34      Disabled  Disabled    Enabled   Disabled 0:0:1:0
200     Disabled  Disabled    Enabled   Disabled 0:0:1:0
1002    Enabled   Enabled     Enabled   Disabled 0:0:1:0
1003    Enabled   Enabled     Enabled   Disabled 0:0:1:0
1004    Enabled   Enabled     Enabled   Disabled 0:0:1:0
1005    Enabled   Enabled     Enabled   Disabled 0:0:1:0

Index  MGID                               (S, G, V)
-----
```

# show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

**show ip pim autorp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** auto-rp is enabled by default.

**Command Modes** Privileged EXEC mode

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** This command displays whether auto-rp is enabled or disabled.

**Examples** The following command output displays that auto-rp is enabled:

```
Switch# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

# show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

**show ip pim bsr-router**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC  
Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** In addition to auto-rp, the BSR RP method can be configured. After the BSR RP method is configured, this command will display the BSR router information.

**Examples** The following is sample output from the **show ip pim bsr-router** command:

```
Switch# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

# show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

**show ip pim bsr**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** In addition to auto-rp, the BSR RP method can be configured. After the BSR RP method is configured, this command will display the BSR router information.

**Examples** The following is sample output from the **show ip pim bsr** command:

```
Switch# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

# show ip pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and decapsulation tunnels on an interface, use the **show ip pim tunnel** command.

```
show ip pim [vrf vrf-name] tunnel [Tunnel interface-number | verbose]
```

## Syntax Description

<b>vrf</b> <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
<b>Tunnel</b> <i>interface-number</i>	(Optional) Specifies the tunnel interface number.
<b>verbose</b>	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

Use the **show ip pim tunnel** to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel)

The PIM Encap Tunnel is dynamically created whenever a group-to-rendezvous point (RP) mapping is learned (through auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop designated routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created—but it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.



### Note

PIM tunnels will not appear in the running configuration.

The following syslog message appears when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

## Examples

The following is sample output from the **show ip pim tunnel** taken from an RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP:

```
Switch# show ip pim tunnel
```

```
Tunnel0
  Type   : PIM Encap
  RP     : 70.70.70.1*
  Source : 70.70.70.1
Tunnel1*
  Type   : PIM Decap
  RP     : 70.70.70.1*
  Source : -R2#
```



---

**Note**

The asterisk (\*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

---



# show mdns cache

To display mDNS cache information for the switch, use the **show mdns cache** privileged EXEC command.

**show mdns cache** [*interface type number* | *name record-name* [*type record-type*] | *type record-type*]

## Syntax Description

<b>interface</b> <i>type-number</i>	(Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.
<b>name</b> <i>record-name</i>	(Optional) Specifies a particular name for which mDNS cache information is to be displayed.
<b>type</b> <i>record-type</i>	(Optional) Specifies a particular type for which mDNS cache information is to be displayed.

## Command Default

None

## Command Modes

Privileged EXEC

User EXEC

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

## Examples

This is an example of output from the **show mdns cache** command without any keywords:

```
Switch# show mdns cache
```

```

[<NAME>]                               [<TYPE>] [<CLASS>] [<TTL>/Remaining] [Accessed] [If-name] [Mac
Address] [<RR Record Data>]
_ airplay._tcp.local                    PTR      IN      4500/4455      0      V1121
b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local
CAMPUS APPLE TV1._airplay._tcp.local SRV      IN      120/75        2      V1121
b878.2e33.c7c5 CAMPUS-APPLE-TV1.local
CAMPUS-APPLE-TV1.local                  A        IN      120/75        2      V1121
b878.2e33.c7c5 121.1.0.254
CAMPUS APPLE TV1._airplay._tcp.local TXT      IN      4500/4455      2      V1121
b878.2e33.c7c5 (I62) 'deviceid=B8:78:2E:33:C7:C6'
```

## show mdns cache

```

      'features=0x5a7ffff7''flags=0x4'
      'model=AppleT~'~
_ipp._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._ipp._tcp.local
EPSON XP-400 Series._ipp._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local
EPSONC053AA.local A IN 120/85 2 V12
2894.0fed.447f 121.1.0.251
EPSON XP-400 Series._ipp._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (384)'txtVers=1' N XP-400 Series' 'usbFG=EPSON''usb_MDL=XP~'~
_smb._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._smb._tcp.local
EPSON XP-400 Series._smb._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local
EPSON XP-400 Series._smb._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (1)'T R2-Access1#

```

# show mdns requests

To display information for outstanding mDNS requests, including record name and record type information, for the switch, use the **show mdns requests** privileged EXEC command.

**show mdns requests** [**detail** | **name** *record-name* | **type** *record-type* [ **name** *record-name* ]]

Syntax Description		
	<b>detail</b>	Displays detailed mDNS requests information.
	<b>name</b> <i>record-name</i>	Displays detailed mDNS requests information based on name.
	<b>type</b> <i>record-type</i>	Displays detailed mDNS requests information based on type.

**Command Default** None

**Command Modes** Privileged EXEC  
User EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

**Examples** This is an example of output from the **show mdns requests** command without any keywords:

```
Switch# show mdns requests
MDNS Outstanding Requests
=====
Request name  :  _airplay._tcp.local
Request type  :  PTR
Request class :  IN
-----
Request name  :  *.*
Request type  :  PTR
Request class :  IN
```

## show mdns statistics

To display mDNS statistics for the switch, use the **show mdns statistics** privileged EXEC command.

```
show mdns statistics {all | service-list list-name | service-policy {all | interface type-number }}
```

### Syntax Description

<b>all</b>	Displays the service policy, service list, and interface information.
<b>service-list</b> <i>list-name</i>	Displays the service list information.
<b>service-policy</b>	Displays the service policy information.
<b>interface</b> <i>type number</i>	Displays interface information.

### Command Default

None

### Command Modes

Privileged EXEC  
User EXEC

### Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

### Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

### Examples

This is an example of output from the **show mdns statistics all** command:

```
Switch# show mdns statistics all
mDNS Statistics
mDNS packets sent      : 0
mDNS packets received  : 0
mDNS packets dropped   : 0
mDNS cache memory in use: 64224(bytes)
```

# show platform ip multicast

To display platform-dependent IP multicast tables and other information, use the **show platform ip multicast** privileged EXEC command.

**show platform ip multicast** {groups | hardware [detail] | interfaces | retry}

Syntax Description		
	<b>groups</b>	Displays IP multicast routes per group.
	<b>hardware [detail]</b>	Displays IP multicast routes loaded into hardware. The optional <b>detail</b> keyword is used to show port members in the destination index and route index.
	<b>interfaces</b>	Displays IP multicast interfaces.
	<b>retry</b>	Displays the IP multicast routes in the retry queue.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

**Examples** This example shows how to display platform IP multicast routes per group:

```
Switch# show platform ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6 flags: C
No RPF interface.
Number of OIF: 0
Flags: 0x10 Pkts : 0
OIF Details:No OIF interface.

DI details
-----
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6 index1:0x51f6

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0
```

## show platform ip multicast

```
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
```

```
Detailed Resource Information (ASIC# 0)
```

```
-----
```

```
al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0
```

```
al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
```

```
Detailed Resource Information (ASIC# 1)
```

```
-----
```

```
al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0
```

```
al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
```

```
=====
```

```
RI details
```

```
-----
```

```
SI details
```

```
-----
```

```
RM:generic lbl = 0x0
RM:di_handle = 0x51f6
RM:fd_const lbl = 0x0
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1
```

```

=====
HTM details
-----
Handle:0x5d604490 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4_Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x5d604518 handle1:0x5d604580

Detailed Resource Information (ASIC# 0)
-----
Number of HTM Entries: 1

Entry #0: (handle 0x5d604518)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
-----
Number of HTM Entries: 1

Entry #0: (handle 0x5d604580)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0

=====

MROUTE ENTRY vrf 0 (*, 224.0.1.40)
Token: 0x0000001f8 flags: C IC
RPF interface: V1121(74238750229529173)): SVI
Token:0x00000021 flags: F IC NS
Number of OIF: 1
Flags: 0x10 Pkts : 0
OIF Details:
      V1121      F IC NS
DI details
-----
Handle:0x603d0000 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4_Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f7 index1:0x51f7

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xe0 0x0 0x1 0x28 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
-----

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

```

## show platform ip multicast

```

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

```

```

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

```

```

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

```

```

=====
RI details
-----

```

```

SI details
-----

```

```

RM:generic lbl = 0x0
RM:di_handle = 0x51f7
RM:fd_const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x1
RM:remote data = 0x1

```

```

=====
HTM details
-----

```

```

Handle:0x603d0440 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x603cfae0 sm handle 0:0x603d0590 handle1:0x603d0520
sm handle 1:0x603d1770

```

```

Detailed Resource Information (ASIC# 0)
-----

```

```

Number of HTM Entries: 1

```

```

Entry #0: (handle 0x603cfae0)

```



```

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
-----
Number of HTM Entries: 1

Entry #0: (handle 0x603d0520)

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0
=====

MROUTE ENTRY vrf 0 (*, 239.255.255.250)
Token: 0x0000003b7d flags: C
No RPF interface.
Number of OIF: 1
Flags: 0x10 Pkts : 95
OIF Details:
    Vl131      F NS
DI details
-----
Handle:0x606ffba0 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f8 index1:0x51f8

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xef 0xff 0xff 0xfa 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
-----

al_rsc_di
RM:index = 0x51f8
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

al_rsc_di
RM:index = 0x51f8
RM:pmap = 0x0

```

## show platform ip multicast

```

RM:cmi = 0x0
RM:rcp_pmap = 0x1
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

```

```

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

```

```

=====
RI details
-----

```

```

ASIC# 0
Replication list :
-----

```

```

Total #ri : 0
start_ri : 15
common_ret : 0

```

```

ASIC# 1
Replication list :
-----

```

```

Total #ri : 6
start_ri : 15
common_ret : 0

```

```

Replication entry rep_ri 0xF #elem = 1
0) ri[0]=50 port=58 dirty=0

```

```

ASIC# 2
Replication list :
-----

```

```

Total #ri : 0
start_ri : 0
common_ret : 0

```

```

SI details
-----

```

```

RM:generic lbl = 0x0
RM:di_handle = 0x51f8
RM:fd_const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp_serviceid = 0x0
RM:dejavu_prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1

```

```

=====
HTM details
-----

```

```

Handle:0x606ff6f8 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x606ff3e0 sm handle 0:0x60ab9160 handle1:0x606ff378
sm handle 1:0x60ab6cc0

```

```

Detailed Resource Information (ASIC# 0)
-----

```

```

Number of HTM Entries: 1

```

```

Entry #0: (handle 0x606ff3e0)

```

```

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

```

```

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0

```

```

Detailed Resource Information (ASIC# 1)
-----

```

```

Number of HTM Entries: 1

```

```

Entry #0: (handle 0x606ff378)

```

```

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

```

```

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0

```

```

=====

```

# wireless mdns-bridging

To enable Ethernet mDNS support, use the **wireless mdns-bridging** command. To disable Ethernet mDNS support, use the **no** form of this command.

**wireless mdns-bridging**

**no wireless mdns-bridging**

This command has no keywords or arguments.

**Command Default** Ethernet mDNS support is enabled by default.

**Command Modes** Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

**Usage Guidelines** Use this command only if you have enabled wireless multicast.

## Examples

This example shows how to enable Ethernet mDNS support:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wireless mdns-bridging
```

# wireless multicast

To enable Ethernet multicast support, use the **wireless multicast** command.

**wireless multicast** [**non-ip** [vlan *vlan-id*]]

## Syntax Description

<b>non-ip</b>	(Optional) Configures multicast non-IP support.
<b>vlan <i>vlan-id</i></b>	(Optional) Specifies multicast non-IP for a VLAN. The interface number ranges between 1 and 4095.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

## Usage Guidelines

None

## Examples

This example shows how to configure multicast non-IP VLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wireless multicast non-ip vlan 20
```





## INDEX

### C

cache-memory-max command [15](#)  
clear ip mfib command [16](#)  
clear ip mroute command [17](#)

### I

ip igmp snooping last-member-query-count command [25](#)  
ip multicast auto-enable command [33](#)  
ip multicast vlan command [34](#)

### R

redistribute mdns-sd command [48](#)

### S

service-list mdns-sd service-list-name command [49](#)  
service-policy command [53](#)  
service-policy-query command [51](#)  
service-routing mdns-sd command [52](#)  
show ip igmp snooping igmpv2-tracking command [60](#)  
show ip igmp snooping wireless mcast-spi-count command [64](#)  
show ip igmp snooping wireless mgid command [65](#)  
show ip pim autorp command [66](#)  
show ip pim bsr command [68](#)  
show ip pim bsr-router command [67](#)  
show ip pim tunnel command [69](#)  
show platform ip multicast command [75](#)

### W

wireless multicast command [83](#)

